COHESITY

5 Reasons Why You Need a Third-party Solution to Back Up Microsoft 365

COHESITY TIPSHEET

5 reasons you need a third-party solution to back up Microsoft 365

Overview

Microsoft 365 (M365) is one of the most widely used office productivity SaaS applications, with nearly 350 million commercial monthly users.[1] But just because M365 files and data live in the cloud doesn't mean they're safe or always available. Your organization needs to ensure you can recover files that may have been deleted from a ransomware attack or a careless employee. Or perhaps you need to meet legal and compliance retention requirements.

Here are the top 5 reasons you need a third-party backup solution to keep your data safe and available whenever you need it.

1. Your enterprise data in the cloud is your responsibility.

Moving to the cloud offloads the headaches associated with on-premises IT infrastructure management, security, and upgrades. Yet it's still up to your IT staff to ensure enterprise data can be recovered at all times and brought back quickly when needed. Microsoft 365 hosts your data in the cloud, but backing it up is your responsibility. Cloud service providers (in this case, Microsoft) focus on service uptime and availability, but as a customer of its cloud service, the onus is on you to safeguard your business data. You need a backup and recovery solution that will protect your data wherever it lives—including in the cloud.

2. Native tools provide limited flexibility for data retention and recovery.

M365's Exchange Online, SharePoint Online, OneDrive, Teams, and Groups come with basic native data retention options, but their flexibility is limited and may not align with your business-level SLAs (for example, deleted email mailboxes are only saved for 30 days). Beyond these basic settings, litigation hold and/or retention policies can be kept as long as needed, but getting the data back can be time consuming and complex. You need to ensure that your backup service has flexibility and provides simple processes for storing and retrieving data to meet your compliance and business needs. A third-party backup service offers greater flexibility, so when you need to restore deleted items to any point in time, you can do so quickly and easily.

Microsoft 365 native protection policies at a glance

Here's how long Microsoft 365 keeps your items by default with their built-in settings:

- Exchange Online
  - 14 days, or up to 30 days if configured
  - 30 days for deleted email boxes
- OneDrive
  - 93 days for site collection Recycle Bin
  - 30 days for a user's Recycle Bin
  - Recovery of data back to a point in time up to 30 days, if configured
- SharePoint
  - 93 days for site collection Recycle Bin
  - 30 days for a user's Recycle Bin
  - Retains backups of deleted items for an additional 14 days
  - Admins can recover deleted site collections and contents up to 90 days
- Teams
  - 1-7 days for messages
  - Other data types have limited retention based on the services providing them

1 Microsoft Earnings Release FY22 Q3

How do you know if your M365 data is at risk? Just because your data lives in the cloud doesn't mean it's safe or always available when you need it most. To ensure you can recover files that were erroneously deleted, meet legal and compliance requirements, or recover from cyber attacks, give yourself peace of mind. Find out the 5 reasons why your business needs a third-party data protection solution to back up Microsoft 365 data.